UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,157	12/21/1999	JAMES H. MOORE	D/99748	3291

7590 11/18/2005

John S. Zanghi Esq.
Fay, Sharpe, Fagan, Minnich & McKee LLP
1100 Superior Avenue
Seventh Floor
Cleveland, OH 44114-2579

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 11/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,157	MOORE, JAMES H.	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3 and 5-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3 and 5-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the papers received on 8/22/2005.

2. **Claims 1, 3, 5 - 16** are pending on this application. Claims 2 and 4 are canceled. Claims 8 - 16 are newly added. **Claims 1, 6, 7** are amended. Independent claim are **1, 11**.

Response to Arguments

3. Applicant's arguments filed **1, 3, 5 - 16** have been fully considered but they are not persuasive.

Response to Remarks

3.1 Applicant argues that the referenced prior art (Haber) does not disclose *" ... the steps of generating Public and Public Key pairs for the client and the Time Source Provider ... " ; " ... using the Key pairs for encrypting and decrypting the data and file attributes ... " (see Remarks Page 7, Lines 6-9) ; " ... Time Source Provider generating its own public/private key pair, whereby the two sets of key pairs are used to encrypt and decrypt the data and file attributes ... " (see Remarks Page 7, Lines 11-13) ; " ... associating the client's Public and Private Key pair an organization, a corporate unit or an individual ... " (see Remarks Page 7, Lines 15-17)*

The Haber (5,136,647) and Romney (6,085,322) prior art combination discloses a client system generating a public and private key pair which is utilized in the encryption and decryption of sensitive data within a network environment. (see Romney Figure 2; col. 6, line 62-63: generation of client public/private key pair utilized for encryption/decryption)

The Haber (5,136,647) and Berson (5,949,879) prior art combination discloses a data center (i.e. an organizationally associated entity) utilized to generate a public and private key pair, which is utilized for the encryption and decryption of data during a communications session. (see Berson col. 4, lines 29-34; col. 5, lines 12-15: generation of public/private key pair, encryption and decryption for data protection)

3.2 Applicant argues that the referenced prior art (Berson) does not disclose " ... *encrypting files with the client's private key and the Time Source Provider's public key and decrypting the files with the Time Source Provider's private key and the client's public key ...* " *(see Remarks Page 7, Lines 27-29)*

The Haber (5,136,647) and Lirov (6,785,810) prior art combination discloses the capability to double encrypt sensitive data utilizing the previously disclosed set of public and private key pair combinations. (see Lirov col. 3, lines 44-46: double encryption of sensitive data utilized combinations of public and private key pairs, encrypt: client private key then TSP public key)

3.3 Applicant argues that the referenced prior art does not disclose " ... *multiple or differing error correcting codes, let alone specific codes for (a) time, (b) time*

source calibration data, (c) file attributes, or (d) encryption key signatures ... " (see Remarks Page 8, Lines 4-5)

The Haber (5,136,647) and Berson (5,949,879) prior art combination discloses differing error codes based on the type of encountered error or format of message data (i.e. time source value). (see Berson col. 9, lines 4-6; col. 9, lines 16-19: differing error codes, communications errors, message format error (i.e. file attributes, part of message format))

3.4 Applicant argues that the referenced prior art does not disclose " ... *mention of a session key ... " (see Remarks Page 8, Line 22)*

The Haber (5,136,647) and Berson (5,949,879) prior art combination discloses the utilization of a session key within a cryptographic system. (see Berson col. 4, lines 35-41; col. 4, lines 42-45: cryptographic session key)

3.5 In reply to an obviousness rejection under 35 U.S.C. § 103, applicant argues that the secondary and primary reference combination is not allowed due to nonobviousness.

The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Furthermore, in response to applicant's arguments against the reference

individually, one cannot show nonobviousness by attacking references individually where rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 103

4. **Claims 1, 3, 5, 6, 8 - 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al. (U.S. Patent No. 5,136,647) in view of Romney et al. (U.S. Patent No. 6,085,322) and further in view of Berson et al. (U.S. Patent No. 5,949,879) and further in view of Lirov et al. (U.S. Patent No. 6,785,810).

Regarding claim 1 (Currently Amended), a method for securing the integrity of files prior to archiving of the files, involving an exchange between a client and a Time Source Provider, the method comprising the steps of:

Haber discloses secure time-stamping of digital documents (see Haber col. 2, lines 33-36) between an agency (i.e. an organizationally associated third party, time source provider) and client, and verify by digital signatures. (see Haber col. 2, line 66 - col. 3, line 1: TSA, time stamp agency (i.e. organizationally associated entity))

Haber does not disclose a client generating a Key pair, the generation of a organizationally associated Public/Private key pair, a client generating attributes

including cryptographic signatures, and private key encryption of file and message digest. However:

a) Romney discloses a client generating a Public/Private Key pair that is associated with an organization, a corporate unit or an individual; (see Romney Figure 2; col. 6, line 62-63) In addition, Berson discloses a client generating a Public/Private Key pair that is associated with an organization, a corporate unit or an individual. (see Berson col. 4, lines 29-34; col. 5, lines 12-15: generation of public/private key pair, encryption and decryption for data protection, data center (i.e. organizationally associated entity))

b) Berson discloses generating an organizationally associated (i.e. certificate attached) public/private key pair for use in transactions with the client; (see Berson col. 4, lines 29-34; col. 5, lines 12-15: generation of public/private key pair, encryption and decryption for data protection, data center (i.e. organizationally associated entity), certificate of authenticity)

c) Romney discloses a client generating a cryptographic signature including attributes of the files that are to be archived, the attributes including files sizes. (see Romney col. 7, lines 51-52) and attached to the document (see Romney col. 7, line 60);

d) Romney discloses encrypting client's files with the client's Private Key and then with the Time Source Provider's Public Key (see Romney col. 8, line 42). In addition, Lirov discloses encrypting client's files with the client's Private Key and then with the Time Source Provider's Public Key. (see Lirov col. 3, lines 44-46:

double encryption of sensitive data utilized combinations of public and private key pairs, encrypt: client private key then TSP public key)

e) Haber discloses a client (i.e. author) converts the digital document to a reduced digital size (see Haber col. 3, line 811) using oneway hash (see Haber col. 3, line 13: digital signature (i.e. hash)) to meet the step of transmitting encrypted data).

f) Berson discloses decrypting the encrypted data and file attributes with private key and then with the client's public key. (see Berson col. 4, lines 4-12: standard public/private key cryptographic techniques utilized, one key (i.e. public or private) is used to encrypt data, the other key is used to decrypt encrypted data) In addition, Lirov discloses decrypting encrypted data with private key then client public key. (see Lirov col. 3, lines 44-46: double encryption of sensitive data utilized combinations of public and private key pairs, decrypt: TSP private key then client public key)

g) Haber discloses a TSA (i.e. Time Source Provider) creating a Time_Map as a time stamp receipt (see Haber Fig. 2, step 25) containing a current time (see Haber col. 4, line 1014), an ID of author, a hash of document, and receipt of the data, etc for each document (see Haber col. 4, line 8: data collection) with a variety of parameters as a string (see Haber col. 6, line 24), and cryptographic signatures. (see Haber col. 6, line 2830: utilized signature techniques);

h) Haber discloses TSA (i.e. time source provider) returning client's data along with certified (i.e. digital signature), TimeMap and encryption key signatures. (see Haber col. 4, line 23; col. 7, line 2)

i) Haber discloses TSA (i.e. time source provider) providing the encrypted client data back to the client (i.e. author). (see Haber step 27; col. 6, line 57; col. 6, line 68)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted data as taught by Romney (see Romney col. 6, lines 62-63), and to generate TSA type cryptographic (public/private) key pairs utilized in data encryption/decryption techniques as taught by Berson, and to incorporate a procedure for the multiple encryption of files with multiple encryption key pairs as taught by Lirov. One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing (see Romney col. 4, lines 32-37: " ... *verification of the authenticity of a digital signature in the absence of a digital certificate ... verifying that a purported owner of a public key in fact has present custody of the corresponding private key at the time a digital signature is executed ...* "), and to employ Berson in order to optimize and enhance procedures in the generation and authentication of digital signatures (see Berson col. 2, line 12-13: " ... *provides for a audit-able, secure environment for the generation of cryptographically protected digital data ...* "), and to employ Lirov in order to provide optimum security and privacy protections without impeding performance (see Lirov col. 2, line 29-33: " ... *system and method that combines security and privacy protection without impeding data processing performance ... in a relational database ...* ").

Regarding claim 3 (Original), Haber discloses wherein to utilize the generation of digital signatures and providing said signatures. (see Haber col. 2, line 66 col. 3, line 5) Haber does not disclose multiple (i.e. double) encryption for data files. However, Lirov discloses wherein the client provides multiple encryption of files. (see Lirov col. 3, lines 44-46: multiple (i.e. double) encryption for data files)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Haber's timestamp signature process to incorporate a procedure for the multiple encryption of files in the generation of digital signatures (see Lirov col. 3, line 44-46) of the encrypted files with encryption keys as taught in Lirov. One would have been motivated to generate encrypt signature keys for preserving the security to employ Lirov in order to provide optimum security and privacy protections without impeding performance. (see Lirov col. 2, line 29-33: " *... system and method that combines security and privacy protection without impeding data processing performance ... in a relational database ...* ").

Regarding claim 5 (Original), Haber discloses sequential numbers, application of representation of the time, and digital signatures. Haber does not disclose the application of multiple nor differing errorcorrecting codes. However, Berson discloses the utilization of a session key for cryptographic techniques, and multiple or differing error correcting codes with source calibration data. (see Berson col. 8, line 59 - col. 9, line 7: error correcting codes for transmission errors) to generate variable values.

It would have been obvious to one of ordinary skill in the art at the time the

invention to modify Haber's to add the session key data transmission with some kind of error detection and correction bits by adapting the error correction codes taught in Berson. One would have been motivated to apply representation of time and error correction codes for correcting differential errors in the detected value in order to prevent a garbled key in data transmission and to produce a precise measure of the key values and ensure the integrity of documentation with an electronic time stamp. (see Berson col. 2, line 12-13)

Regarding claim 6 (Currently Amended), Haber discloses secure time-stamping of digital documents between agency (i.e. time source provider) and client, but Haber does not specifically disclose the client producing said archived files, file attributes and time map; TSA (i.e. time source provider) retrieving time map and session key; regenerating time map; encrypting said time map with said session key and compare them. However, Romney discloses a method as in claim 1, further comprising the steps of:

b) client producing the archived files, file attributes and time map; (see Romney col. 7, lines 1-6: any collection of digital data, authenticator identification envelope consists of file specific information)

c) Time Source Provider retrieving the time map and session key; (see Romney col. 7, lines 30-36: transmit time map)

d) the Time Source Provider regenerating the time map; (see Romney col. 8, line 64 - col. 9, line 4)

e) the Time Source Provider encrypting the time map with the session key; (see Romney col. 11, line 26-28 authenticator identification envelope (i.e. time map))

f) comparing the regenerated time map to the time map. (see Romney col. 5, lines 19-25: utilize standard comparison techniques to verify a digital signature)

Romney does disclose the usage of a session key within a cryptographic system. However, Berson discloses:

a) exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction; (see Berson col. 4, lines 35-41; col. 4, lines 42-45: session key utilized within a cryptographic system)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted data as taught by Romney (see Romney col. 6, lines 62-63), and to generate cryptographic (public/private) key pairs utilized in data encryption/decryption techniques and the usage of a cryptographic session key as taught by Berson. One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing (see Romney col. 4, lines 32-37), and to employ Berson in order to optimize and enhance procedures in the generation and authentication of digital signatures (see Berson col. 2, line 12-13).

Regarding Claims 8, Romney discloses a method as in claim 1, further comprising the steps of:

a) protecting the client's filenames via a filename lookup table having a signature; (see Romney col. 7, lines 1-6: any collection of digital data, file specific information (i.e. filename lookup table))

b) transmitting the signature of the filename lookup table to the Time Source Provider. (see Romney col. 7, lines 30-36: transmit time map)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted sensitive data as taught by Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing. (see Romney col. 4, lines 32-37)

Regarding Claims 9, Romney discloses a method as in claim 1, further comprising the step of: recording in the time map at least one of the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption'keys for data exchange were updated. (see Romney col. 7, lines 1-6: any collection of digital data, time (i.e. clock) specific information, file specific information)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted sensitive data as taught by Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing. (see

Romney col. 4, lines 32-37)

Regarding Claim 10, Romney discloses a method as in claim 9, further comprising the step of: recording in the time map at least one of the list of archived files, the sizes of the archived files, and the signatures of any encrypted files. (see Romney col. 7, lines 1-6: any collection of digital data, file specific information (i.e. file size, list of files))

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted sensitive data as taught by Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing. (see Romney col. 4, lines 32-37)

5. **Claims 7, 11 - 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber-Romney-Berson-Lirov and further in view of Doyle (U.S. Patent No. 6, 381,696).

Regarding claim 7 (Currently Amended), a method as in claim 1, further comprising the steps of:

a) Haber does not disclose clear channel transaction. However, Doyle discloses establishing the clear channel transaction interval and pattern; (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

b) Haber does not disclose the client generating client public/private key pairs. However, Romney discloses a client generating and encrypting data utilizing public/private key pairs; (see Romney col. 2, lines 4-50; col. 7, lines 42-45: public/private key pair) Neither Haber nor Romney discloses clear channel transactions. However, Doyle discloses utilizing the clear (i.e. secure) channel transactions. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

c) Haber discloses transactions between a client and a TSA (i.e. time source provider). (see Haber col. 2, line 66 - col. 3, 1: TSA (i.e. time source provider)) Neither Haber nor Romney discloses clear channel transactions. However, Doyle discloses utilizing the clear (i.e. secure) channel transactions. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

d) Doyle discloses triggering an alarm if said clear channel transaction is not received by the Time Source Provider. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions (an alarm, indication of an error condition is a standard processing procedure during transaction))

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Haber to utilize client public/private cryptographic key pairs as taught in Romney, and to utilized clear (i.e. secure) channel transactions as taught by Doyle. One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize the effectiveness of security in encryption key generation and data processing transactions (see Romney col. 4, lines 32-37), and to

employ Doyle in order to enhance procedures in authentication of a digital signature (see Doyle col. 3, lines 33-37).

Regarding Claim 11, Romney discloses a method for securing the integrity of archived files for a client:

a) establishing a public and private key pair for a client, wherein the client's public and private key pair associated with an organization, a corporate unit or one or more individuals; (see Romney Figure 2; col. 6, line 62-63) In addition, Berson discloses a client generating a Public/Private Key pair that is associated with an organization, a corporate unit or an individual. (see Berson col. 4, lines 29-34; col. 5, lines 12-15: generation of public/private key pair, encryption and decryption for data protection, data center (i.e. organizationally associated entity))

b) generating a public and private key pair for use in transactions with the client; (see Romney Figure 2; col. 6, line 62-63)

e) creating a time map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client; (see Romney col. 8, line 64 - col. 9, line 4)

Haber does not disclose clear channel communications. However, Doyle discloses:

c) receiving a data transmission from the client over a clear channel, wherein the data transmission includes encrypted data and archived file attributes and the client's Public Key signature and wherein the archived file attributes include data

relating to the sizes of the files and cryptographic signatures and the archived files have been encrypted with the client's private key and with the time source provider's public key; (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

f) transmitting the encrypted client data along with the time map and session key signature over the clear channel to the client. (see Doyle col. 7, lines 42-45: secure SSL (i.e. clear channel) transactions)

Haber does not disclose multiple encryption techniques for the encryption of sensitive data. However, Lirov discloses:

d) decrypting the encrypted data and file attributes with the time source provider's private key and then with the client's public key; (see Lirov col. 3, lines 44-46: double encryption of sensitive data utilized combinations of public and private key pairs, decrypt: client public key then TSP private key)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate TSA type cryptographic (public/private) key pairs utilized in data encryption/decryption techniques as taught by Berson, and to generate client public/private key pairs, sign encrypted data as taught by Romney (see Romney col. 6, lines 62-63), and to incorporate a procedure for the multiple encryption of files in the generation of digital signatures of the encrypted files with encryption keys as taught by Lirov, and to utilized clear (i.e. secure) channel transactions as taught by Doyle. One of ordinary skill in the art would be motivated to

employ Berson in order to optimize and enhance procedures in the generation and authentication of digital signatures (see Berson col. 2, line 12-13), and to employ Romney in order to enhance and optimize effective security in encryption key generation and processing (see Romney col. 4, lines 32-37), and to employ Lirov in order to provide optimum security and privacy protections without impeding performance (see Lirov col. 2, line 29-33), and to employ Doyle in order to enhance procedures in authentication of a digital signature (see Doyle col. 3, lines 33-37).

Regarding Claim 12, Romney discloses a method as in claim 11, further comprising the steps of:

a) protecting the client's filenames via a filename lookup table having a signature; (see Romney col. 7, lines 1-6: any collection of digital data, authenticator identification envelope consists of file specific information)

b) transmitting the signature of the filename lookup table to the Time Source Provider. (see Romney col. 7, lines 30-36: transmit time map)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted sensitive data as taught by Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing. (see Romney col. 4, lines 32-37)

Regarding Claim 13, Romney discloses a method as in claim 12, further comprising the step of: recording in the time map at least one of the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption keys for data exchange were updated. (see Romney col. 7, lines 1-6: any collection of digital data, time (i.e. clock) specific information, file specific information)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted sensitive data as taught by Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing. (see Romney col. 4, lines 32-37)

Regarding Claim 14, Romney discloses the method as defined in claim 13, further comprising the step of: recording in the time map at least one of the list of archived files, the sizes of the archived files, and the signatures of any encrypted files. (see Romney col. 7, lines 1-6: any collection of digital data, list of archived files, sizes of files, file specific information)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, sign encrypted sensitive data as taught by Romney. (see Romney col. 6, lines 62-63) One of ordinary skill in the art would be motivated to employ Romney in order to enhance

and optimize effective security in encryption key generation and processing. (see Romney col. 4, lines 32-37)

Regarding Claim 15, Romney discloses the method as defined in claim 14, further comprising the step of:

b) retrieving the time map and session key; (see Romney col. 7, lines 30-36: transmit time map)

c) regenerating the time map; (see Romney col. 8, line 64 - col. 9, line 4)

d) encrypting the time map with the session key; (see Romney col. 11, line 26-28 authenticator identification envelope (i.e. time map)) and

e) comparing the regenerated time map the time map. (see Romney col. 5, lines 19-25: utilize standard comparison techniques to verify a digital signature)

Romney does not disclose the utilization of a session in cryptographic functions. However, Berson discloses:

a) exchanging a session key between the client and the Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction; (see Berson col. 4, lines 35-41; col. 4, lines 42-45: session key utilized within a cryptographic system)

It would have been obvious to one of the ordinary skilled in the art at the time the invention was made to modify Haber to generate client public/private key pairs, generate time map information, sign encrypted sensitive data as taught by Romney (see

Romney col. 6, lines 62-63), and to generate TSA type cryptographic (public/private) key pairs utilized in data encryption/decryption techniques as taught by Berson. One of ordinary skill in the art would be motivated to employ Romney in order to enhance and optimize effective security in encryption key generation and processing (see Romney col. 4, lines 32-37), and to employ Berson in order to optimize and enhance procedures in the generation and authentication of digital signatures (see Berson col. 2, line 12-13).

Regarding Claim 16, Lirov discloses the method defined in claim 15, further comprising the step of: applying multiple or differing error checking codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures. (see Lirov col. 3, lines 44-46: double encryption of sensitive data utilized combinations of public and private key pairs, encrypt: client private key then TSP public key)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Haber timestamp signature process to incorporate a procedure for the multiple encryption of files with multiple encryption key pairs as taught in Lirov. One would have been motivated to generate encrypt signature keys for preserving the security to employ Lirov in order to provide optimum security and privacy protections without impeding performance. (see Lirov col. 2, line 29-33)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

K H S

Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
Nov. 12, 2005

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100